Comment regarding Class-25: Software – security research

Brandon Perry, VolatileMinds

Legislation concerning lawful security research requires consideration not only into the current state of software security, but also the future of how we as Americans will consume and create software. Increasingly, software drives basic functions within each and every American's daily life. Legislators and members of the security community have an excellent opportunity to create a framework that allows research by those with the capabilities and know-how to bolster the security of our homes, our businesses, and our infrastructure.

We live in a digital world now. 30 years ago, when computer software was only beginning to be accepted into the mainstream public, legislators passed the Computer Fraud and Abuse Act. This was before the Internet of Everything was a gleam in anyone's eye, and before the notion of us running out of IP addresses was laughable. Now, we have critical infrastructure, smart home appliances, and even vehicles constantly connected to the Internet, and in early 2011, we exhausted the primary address pool of IPv4 addresses for use on the Internet. The world we live in now is so radically different than in 1986. We must work with our legislators to enact radically different laws that enable individuals the ability to constructively assess the security and stability of the software that drives our lives without fear of reproach or, worse, imprisonment.

I am an independent security researcher. I have found severe vulnerabilities in enterprise-grade software meant to protect our government and our businesses. An unfortunate side-effect of deadlines within software development is testing that should be done before a piece of software is released is not performed. Often times, the software testing that is bypassed to make numbers for a fiscal quarter is the exact testing that could prevent many vulnerabilities from being released to the public to begin with. Currently, within the United States, there is a real lack of skills required by companies to perform this testing with the speed and agility our companies require to make deadlines. These skills are generally not taught at universities, and certainly not in our public school systems.

The only way right now to gain these required skills is for independent computer programmers and hobbyists to spend their own free time "hacking". Projects such as Metasploit, an open source exploit database and development framework, allow our computer programmers to look at how vulnerabilities in software are actively exploited. Ignorance of how these vulnerabilities make their way into software and how to exploit them does not help our industry prevent these vulnerabilities from occurring. If anything, it exacerbates the issue, preventing perfectly capable engineers from learning about the exact defects that they should be trying to prevent.

Let us compare the software industry to another industry which requires a high level of testing and accountability; the automotive industry. How many of us have bought cars that required defects to be fixed after purchase, such as ignition switches, airbags, or brakes? When these defects that could cause material damage are found, national recalls are performed and the makers of the vehicles are held personally accountable. There is no such accountability currently for software companies creating infrastructure-critical software. In fact, many end-user license agreements from software companies

have clauses that defer any kind of responsibility for defects found. By accepting the agreement, you cannot hold the software company accountable for any negligence on their part.

Security researchers auditing software for vulnerabilities should be held to high standards, but only if the companies releasing the software are held to high standards as well. It should go without saying that any effort we take now will pay in dividends later if we take the problems that face us in regards to our constantly connected world seriously. We have the knowledge and the expertise to not only craft legislation that begins to have an immediate impact on the safety and security of our homes, businesses, and infrastructure, but takes into account where we are headed as a society that is networked in ways never fathomed during the birth of our industry. We can create a framework that should be a model for other countries to follow that lets us utilize the expertise in software and network systems around the globe to make our lives safe and secure.